Networks don’t lie

Incident started at ISP and almost stroke its customer’s OT

FLOWCUTTER

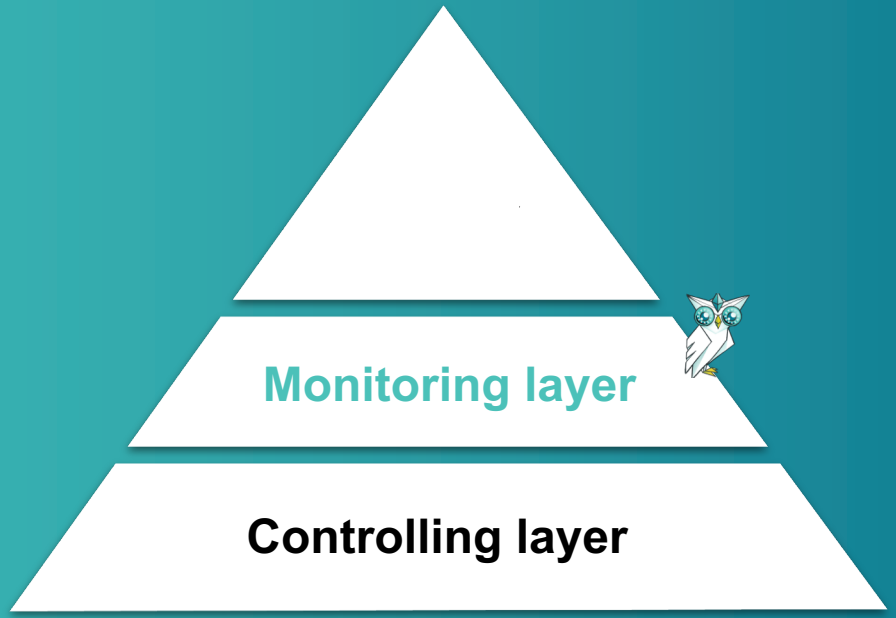
Mgr. Matej Pavelka PhD.

Networks don’t lie

- Network as Source of truth
- Incident to illustrate Best practices
- Role of ISP in SME security

pyra-mid

Security Systems



FLOWCUTTER

a case - incident

Disclaimer
Anonymized
Synthetic

However
Preplicated
Illustrative
More common issue than you think

FLOWCUTTER

Template

- **MITRE ATT&CK®** *https://attack.mitre.org*
- **Tools attackers use**
- **Detection**
- **Mitigation & Improvement**

MITRE | ATT&CK®

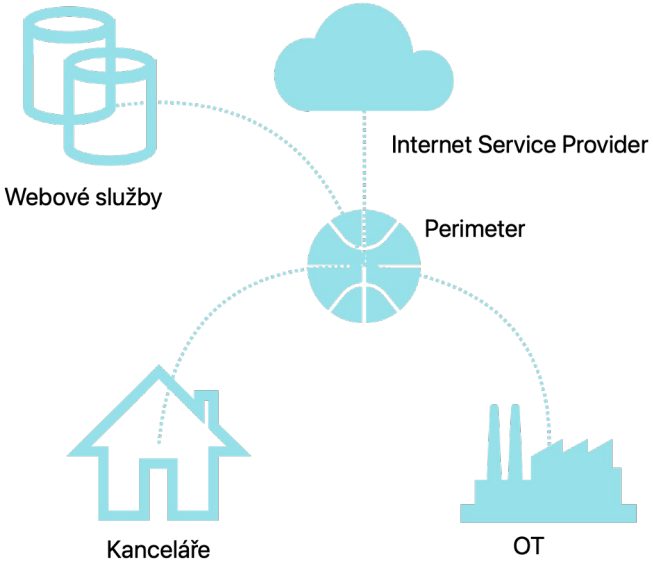
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)	Adversary-in-the-Middle (3)
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization	Debugger Evasion	Forced Authentication
Phishing for Information (4)	Establish Accounts (3)			Compromise		Deobfuscate/Decode Files or Information	
						Deploy Container	

Incident timeline

- Step 1
- Step 2
- Step 3
- Step 4
- Step 5
- Step 6

SME

- 700 hosts (offices, servers, in VLANs)
- Office behind firewall
- Web & other servers hosted by ISP
- Small but important OT



#1 step - recon

of ISP’s public facing IP range

FLOWCUTTER

Incident timeline

- Step 1 - Recon on ISP
- Step 2
- Step 3
- Step 4
- Step 5
- Step 6

Reconnaissance

Before “Spray & Pray”

1) Scan open ports
2) Scan for services
3) Application version

Reconnaissance 10 techniques		Resource 8 te
Active Scanning (3)	II	Acquire Access
Gather Victim Host Information (4)	II	Acquire Infrastructure (8)
Gather Victim Identity Information (3)	II	Compromise Accounts (3)
Gather Victim Network Information (6)	II	Compromise Infrastructure (7)
Gather Victim Org Information (4)	II	Develop Capabilities (4)
Phishing for Information (4)	II	Establish Accounts (3)
Search Closed Sources (2)	II	Obtain Capabilities (6)
Search Open Technical Databases (5)	II	Stage Capabilities (6)
Search Open Websites/Domains (3)	II	
Search Victim-Owned Websites		

Reconnaissance

Before “Spray & Pray”

1) Scan open ports
2) Scan for services
3) Application version

Tooling

- Nessus
- Metasploit
- Vuls
- Archery
- w3af

Reconnaissance 10 techniques	Resource 8 te
Active Scanning (3)	Acquire Access
Gather Victim Host Information (4)	Acquire Infrastructure (8)
Gather Victim Identity Information (3)	Compromise Accounts (3)
Gather Victim Network Information (6)	Compromise Infrastructure (7)
Gather Victim Org Information (4)	Develop Capabilities (4)
Phishing for Information (4)	Establish Accounts (3)
Search Closed Sources (2)	Obtain Capabilities (6)
Search Open Technical Databases (5)	Stage Capabilities (6)
Search Open Websites/Domains (3)	
Search Victim-Owned Websites	

Reconnaissance

- Before “Spray & Pray”
  1) Scan open ports
  2) Scan for services
  3) Application version
- Tooling
- How to detect?

Reconnaissance 10 techniques	Resource 8 te
Active Scanning (3)	Acquire Access
Gather Victim Host Information (4)	Acquire Infrastructure (8)
Gather Victim Identity Information (3)	Compromise Accounts (3)
Gather Victim Network Information (6)	Compromise Infrastructure (7)
Gather Victim Org Information (4)	Develop Capabilities (4)
Phishing for Information (4)	Establish Accounts (3)
Search Closed Sources (2)	Obtain Capabilities (6)
Search Open Technical Databases (5)	Stage Capabilities (6)
Search Open Websites/Domains (3)	
Search Victim-Owned Websites	

netflow

RFC 3954 & RFC 7011

Photo from internet.org

FLOWCUTTER

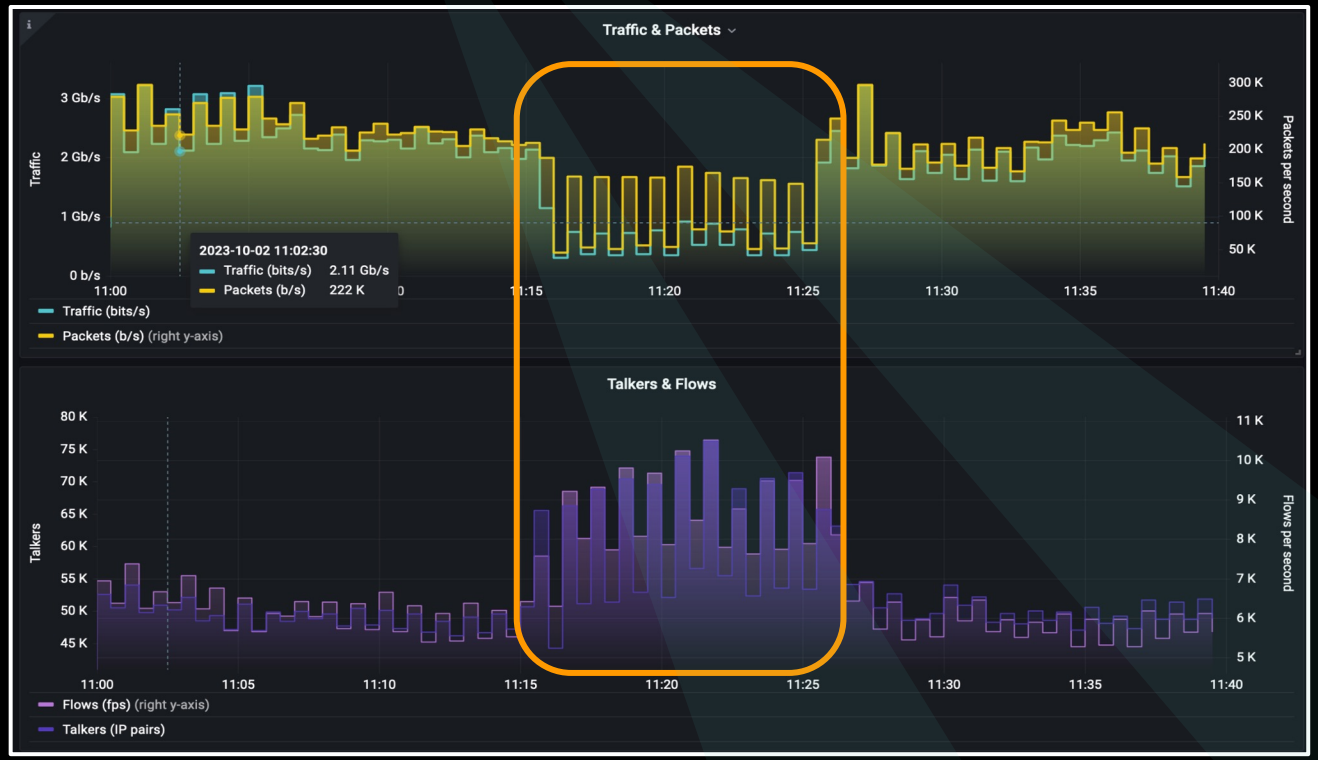
Example flow record

- L4 protocol: **TCP**
- Source IP: **10.2.3.44**
- Source port: 12345
- Destination IP
- Destination port: **443**
- TCP flags: **SYN, ACK**

- Can be enriched for example by L7 application layer or JA3 fingerprints

Net traffic

All traffic BPS, PPS, FPS, talkers

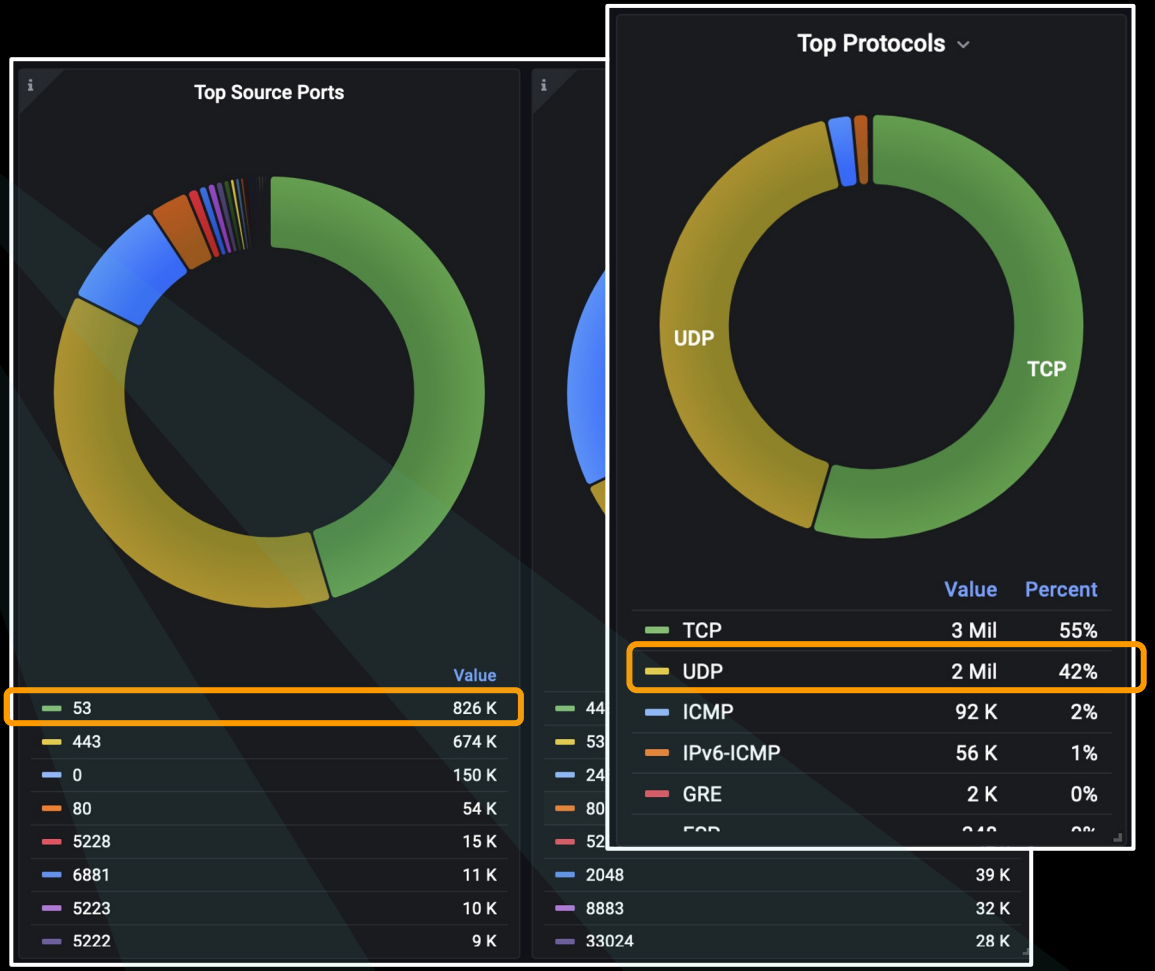


10 minutes

FLOWCUTTER

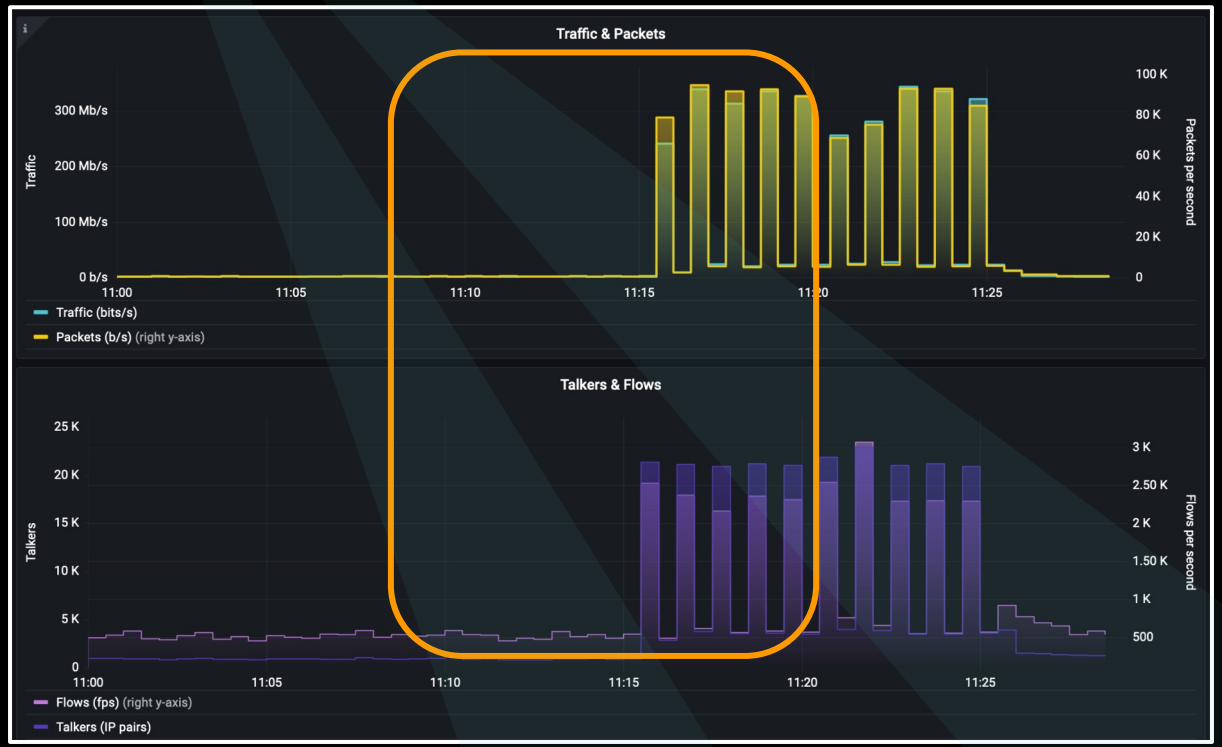
Drill down

- DNS responses
- Source port = 53



DNS responses

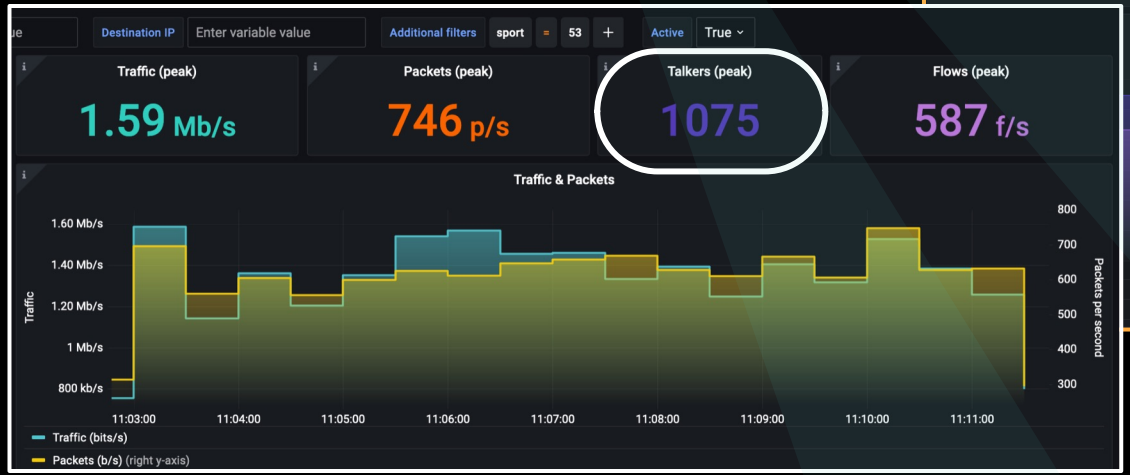
Filtered source_port = 53



Before / after

During attack

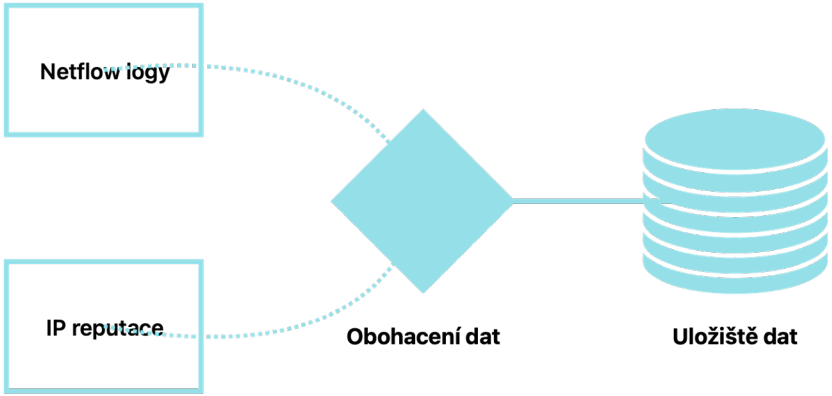
Before attack



FLOWCUTTER

Scanner Detection

- Possibly from Netflow
- Easier for ISP w/ large IP range
- How to improve confidence?
- Multiple data sources
- Firewall w/ dynamic feed



#2 step - initial access

to ISP’s CORE router

FLOWCUTTER

Incident timeline

- Step 1 - Recon on ISP
- Step 2 - Access to ISP router
- Step 3
- Step 4
- Step 5
- Step 6

ISP infrastructure

- Small ISP ~ 8000 connections
- Avg of 22K netflow records per second
- CORE routers (RouterOS) on perimeter

CVE-2022-45315

Mikrotik RouterOs before stable v7.6 was discovered to contain an out-of-bounds read in the SNMP process. This vulnerability allows attackers to execute arbitrary code via a crafted packet.

22K

Initial access

- **RouterOS vulnerability**

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
9 techniques	9 techniques	17 techniques	12 techniques	23 techniques	15 techniques
Content Injection	Command and Scripting Interpreter (4)	Account Manipulation (1)	Abuse Elevation Control Mechanism (2)	Abuse Elevation Control Mechanism (2)	Adversary-in-the-Middle (2)
Drive-by Compromise	Exploitation for Client Execution	Boot or Logon Autostart Execution (2)	Account Manipulation (1)	Debugger Evasion	Brute Force (4)
Exploit Public-Facing Application	Inter-Process Communication	Boot or Logon Initialization Scripts (1)	Boot or Logon Autostart Execution (2)	Deobfuscate/Decode Files or Information	Credentials from Password Stores (3)
External Remote Services	Native API	Browser Extensions	Boot or Logon Initialization Scripts (1)	Execution Guardrails (1)	Exploitation for Credential Access
Hardware Additions	Scheduled Task/Job (3)	Compromise Client Software Binary	Create or Modify System Process (1)	Exploitation for Defense Evasion	Forge Web Credentials (1)
Phishing (4)	Shared Modules	Create Account (2)	Escape to Host	File and Directory Permissions Modification (1)	Input Capture (3)
Supply Chain Compromise (3)	Software Deployment Tools	Create or Modify System Process (1)	Event Triggered Execution (3)	Hide Artifacts (8)	Modify Authentication Process (2)
Trusted Relationship	System Services	Event Triggered Execution (3)	Exploitation for Privilege Escalation	Hijack Execution Flow (2)	Multi-Factor Authentication Interception
Valid Accounts (3)	User Execution (2)			Impair Defenses (7)	
				Impersonation	
				Indicator Removal (7)	

Attack Detection

- **NOT just from Netflow**
- **How to improve posture?**
- **Close mng. ports to internet**
- **How to improve detection confidence?**
- **Multiple data sources**

1. Vulnerability scan discovery for CORE,
2. Incoming packets to ports related to discovered vulnerabilities,
3. attacker is on IP deny list.

Vulnerability discovery

Number of findings	High severity	Medium severity	Low severity	Log severity	Most of the findings:	Most visited CVE
302	2	15	17	21	10.30.3.14	CVE-2020-25073

TOP 10 IP

IP	Count
10.30.3.14	42
10.10.1.15	36
10.10.1.13	35

TOP 10 CVEs

CVEs	Description	Number of findings
CVE-2020-25073	Apache HTTP Server /server-status acce...	2
CVE-2011-3389,C...	SSL/TLS: Deprecated TLSv1.0 and TLSv1....	2
CVE-1999-0632	RPC Portmapper Service Detection (TCP)	2
CVE-2010-0020,C...	Microsoft Windows SMB Server NTLM Mu...	1
CVE-2017-0143,C...	Microsoft Windows SMB Server Multiple ...	1

TOP 10 open ports

Port	Count
443	120
22	87
80	42

TOP OS

OS	pocet
Linux 2.6.32	16
Linux 3.2 - 4.9	2
AVtech Room Alert 26W environmental monitor	1
FreeBSD 6.2-RELEASE	1
Linux 2.6.32 - 3.10	1
Linux 2.6.32 - 3.13	1
Microsoft Windows Server 2008 or 2008 Beta 3	1

TOP Ports

Port	Count
22	21
443	7
80	7
139	6
3389	6
445	6
8080	6
135	5
3306	4
53	4

TOP Services

Service	Count
ssh	21
http	14
ms-wbt-server	6
netbios-ssn	6
http-proxy	5
microsoft-ds	5
msrpc	5
rtsp	5
tcpwrapped	5
domain	4

Number of DHCP s...

1

IP	Hostname	Protocol	Port	Severity	CVEs	CVSS ↓	Description	Timestamp
10.10.1.14		tcp	445	High	CVE-2010-0020,CVE-201...	10	Microsoft Windows SMB Server ...	2023-12-14T06:00:33Z
10.10.1.14		tcp	445	High	CVE-2017-0143,CVE-201...	8.10	Microsoft Windows SMB Server ...	2023-12-14T06:00:33Z
10.30.3.14		tcp	443	Medium	CVE-2020-25073	5.30	Apache HTTP Server /server-stat...	2023-12-14T06:00:33Z
10.30.3.14		tcp	80	Medium	CVE-2020-25073	5.30	Apache HTTP Server /server-stat...	2023-12-14T06:00:33Z

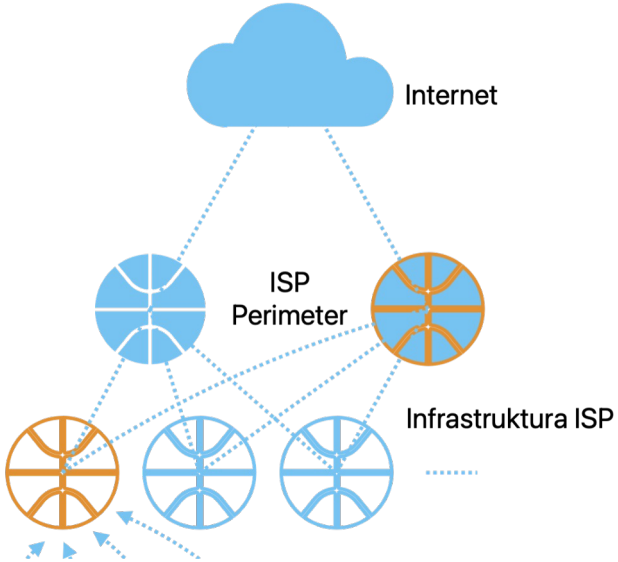
#3 step - lateral movement

within ISP’s infrastructure

FLOWCUTTER

Incident timeline

- Step 1 - Recon on ISP
- Step 2 - Access to ISP router
- Step 3 - Lateral movement within ISP
- Step 4
- Step 5
- Step 6



Lateral movement

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
9 techniques	9 techniques	17 techniques	12 techniques	23 techniques	15 techniques	23 techniques	7 techniques
Content Injection	Command and Scripting Interpreter (4)	Account Manipulation (1)	Abuse Elevation Control Mechanism (2)	Abuse Elevation Control Mechanism (2)	Adversary-in-the-Middle (2)	Account Discovery (2)	Exploitation of Remote Services
Drive-by Compromise	Exploitation for Client Execution	Boot or Logon Autostart Execution (2)	Account Manipulation (1)	Debugger Evasion	Brute Force (4)	Application Window Discovery	Internal Spearphishing
Exploit Public-Facing Application	Inter-Process Communication	Boot or Logon Initialization Scripts (1)	Boot or Logon Autostart Execution (2)	Deobfuscate/Decode Files or Information	Credentials from Password Stores (3)	Browser Information Discovery	Lateral Tool Transfer
External Remote Services	Native API	Browser Extensions	Boot or Logon Initialization Scripts (1)	Execution Guardrails (1)	Exploitation for Credential Access	Debugger Evasion	Remote Service Session Hijacking (1)
Hardware Additions	Scheduled Task/Job (3)	Compromise Client Software Binary	Create or Modify System Process (1)	Exploitation for Defense Evasion	Forge Web Credentials (1)	Device Driver Discovery	Remote Services (2)
Phishing (4)	Shared Modules	Create Account (2)	Escape to Host	File and Directory Permissions Modification (1)	Input Capture (3)	File and Directory Discovery	Software Deployment Tools
Supply Chain Compromise (3)	Software Deployment Tools	Create or Modify System Process (1)	Event Triggered Execution (3)	Hide Artifacts (8)	Modify Authentication Process (2)	Log Enumeration	Taint Shared Content
Trusted Relationship	System Services	Event Triggered Execution (3)	Exploitation for Privilege Escalation	Hijack Execution Flow (2)	Multi-Factor Authentication Interception	Network Service Discovery	
Valid Accounts (3)	User Execution (2)			Impair Defenses (7)		Network Share Discovery	
				Impersonation		Network Sniffing	
				Indicator Removal (7)		Password Policy Discovery	

Lateral movement

How to spread infection

1) Scan open services on local net
2) Try default credentials
3) Try brute-force

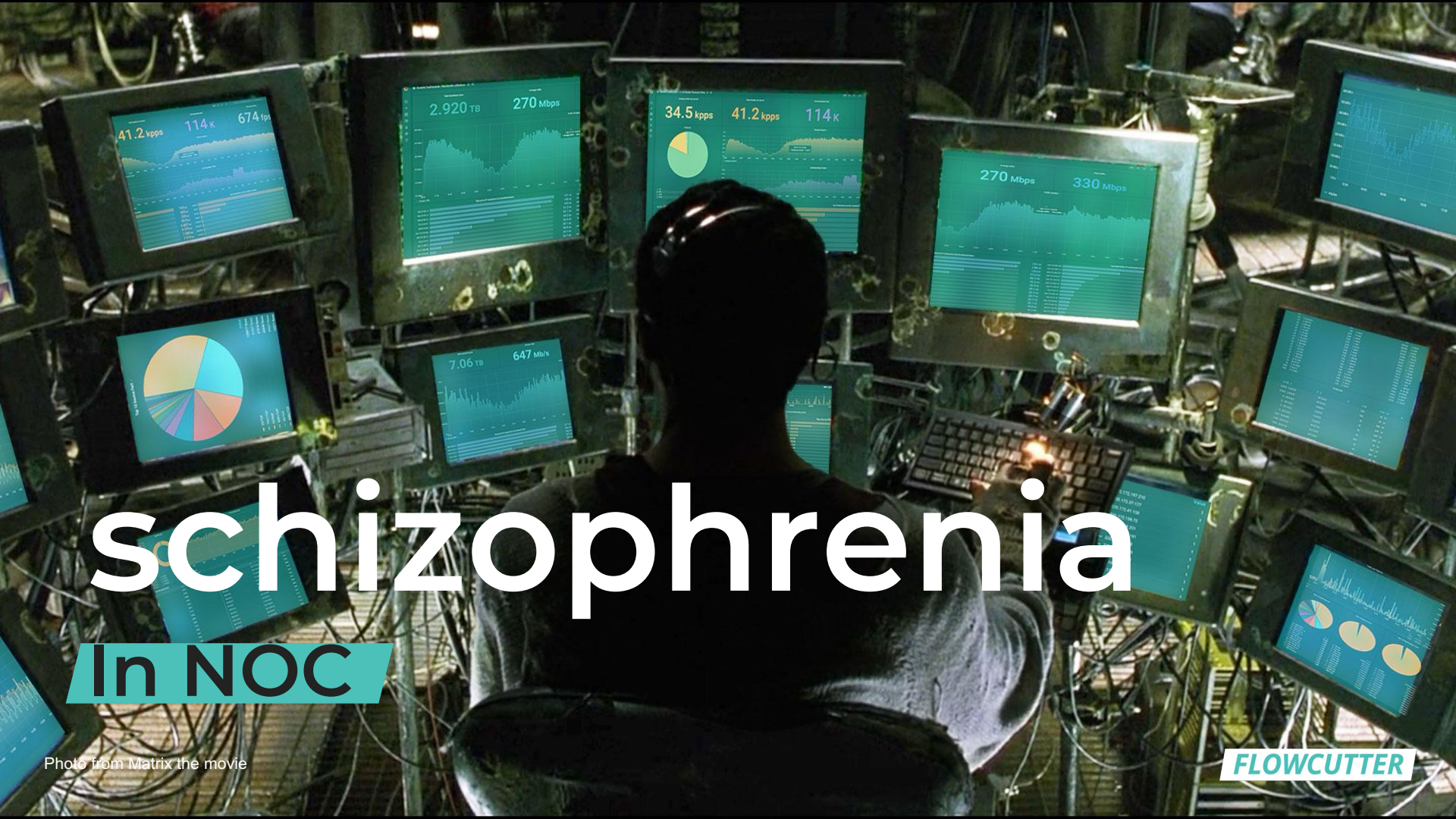
Credential Access	Discovery	Lateral Movement
15 techniques	23 techniques	7 techniques
Adversary-in-the-Middle (2)	Account Discovery (2)	Exploitation of Remote Services
Brute Force (4)	Application Window Discovery	Internal Spearphishing
Credentials from Password Stores (3)	Browser Information Discovery	Lateral Tool Transfer
Exploitation for Credential Access	Debugger Evasion	Remote Service Session Hijacking (1)
Forge Web Credentials (1)	Device Driver Discovery	Remote Services (2)
Input Capture (3)	File and Directory Discovery	Software Deployment Tools
Modify Authentication Process (2)	Log Enumeration	Taint Shared Content
Multi-Factor Authentication Interception	Network Service Discovery	
	Network Share Discovery	
	Network Sniffing	
	Password Policy Discovery	

Brute-force Detection

- Noisy attack
- Easy to detect from Netflow

Netflow visualization

FLOWCUTTER



schizophrenia

In NOC

Photo from Matrix the movie

FLOWCUTTER

Photo from twitter.com/billydracula/

vendor lock

OSS, exporters

Photo from www.geocaching.com

FLOWCUTTER

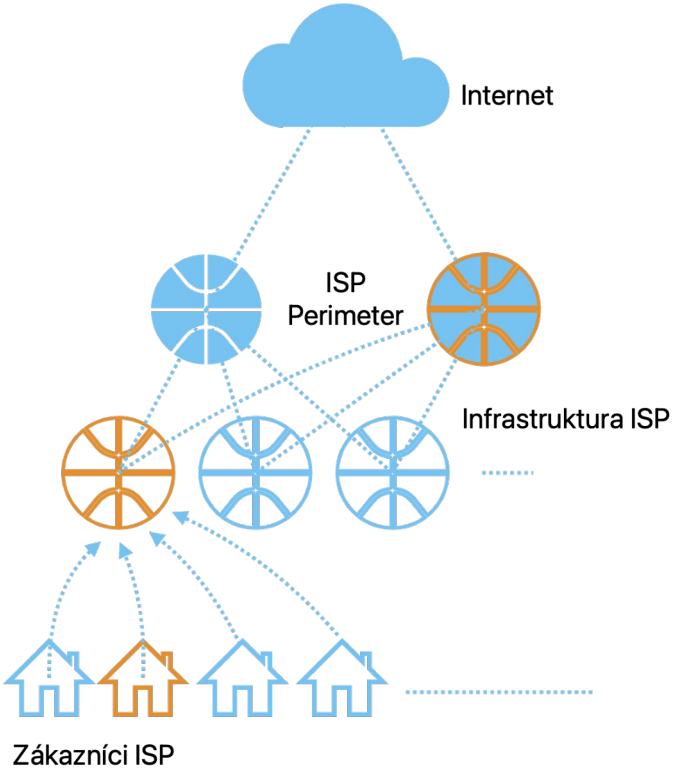
#4 step - infection spreads

to SME

FLOWCUTTER

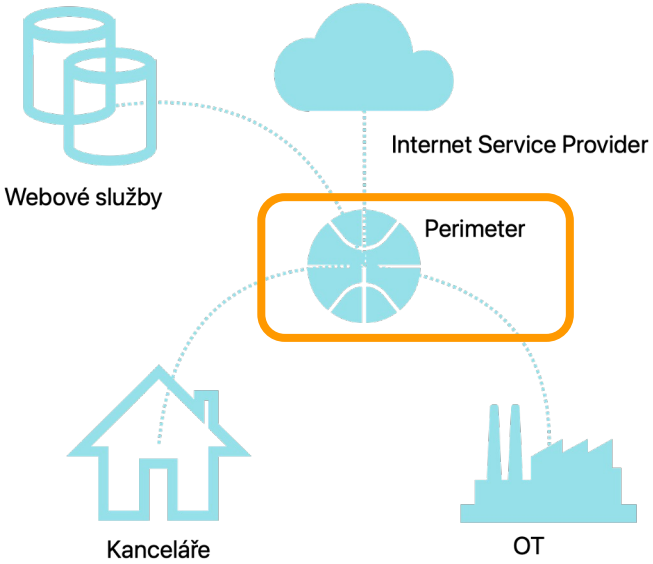
Incident timeline

- Step 1 - Recon on ISP
- Step 2 - Access to ISP router
- Step 3 - Lateral movement within ISP
- Step 4 - Lateral movement to SME
- Step 5
- Step 6



Attacker gains visibility

- Ignoring firewall
- Visibility to all office hosts
- to servers hosted by ISP
- to OT perimeter

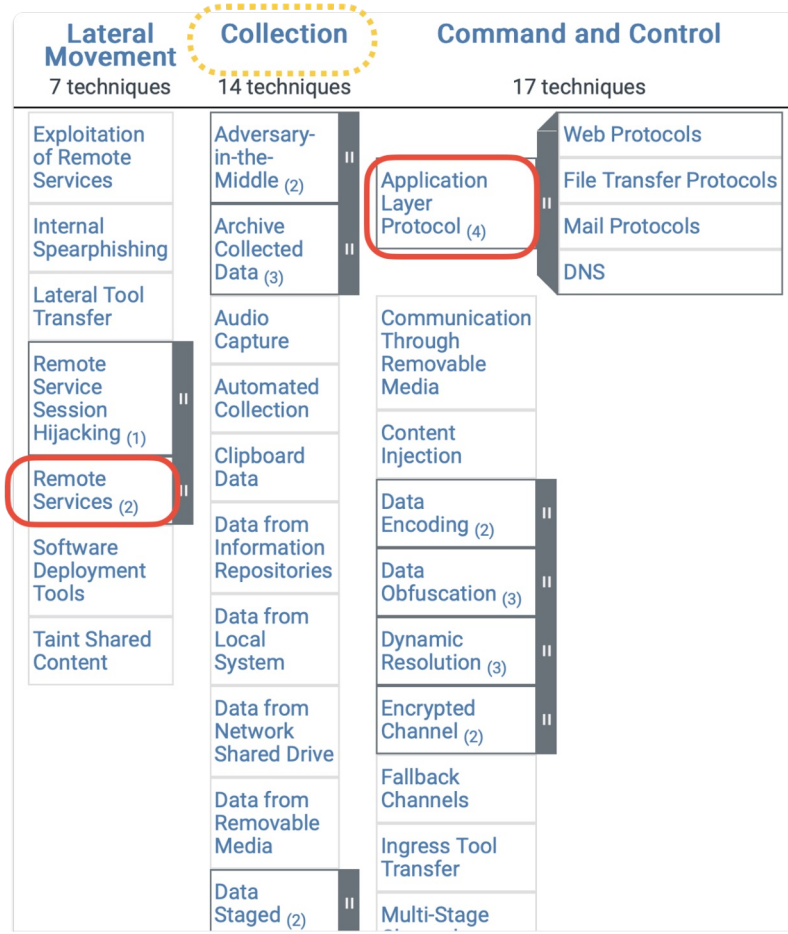


Incident timeline

- Step 1 - Recon on ISP
- Step 2 - Access to ISP router
- Step 3 - Lateral movement within ISP
- Step 4 - Lateral movement to SME
- Step 5 - C2 communication
- Step 6

C2 communication

- Infected router attempts to contact C2
- First via DNS resolving
- Then directly to IP



C2 detection & mitigation

- Not reliable from just NetFlow
- How to improve detection confidence?
- Combine Netflow with IP list of known C2
- C2 hosts resolving can be stopped by DNS security solution

DNS security dashboard

FLOWCUTTER

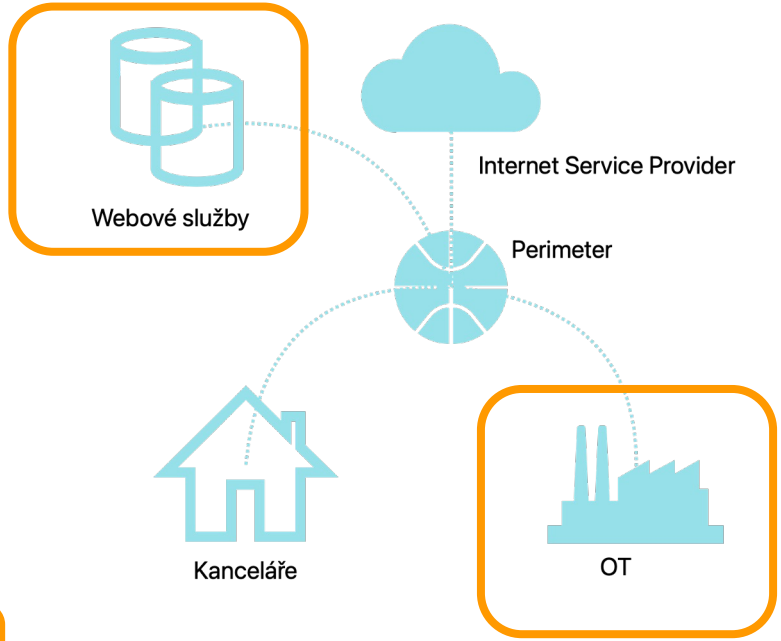
#6 step - attack on OT

and Database server

FLOWCUTTER

Incident timeline

- Step 1 - Recon on ISP
- Step 2 - Access to ISP router
- Step 3 - Lateral movement within ISP
- Step 4 - Lateral movement to SME
- Step 5 - C2 communication
- Step 6 - Attack on OT & db server



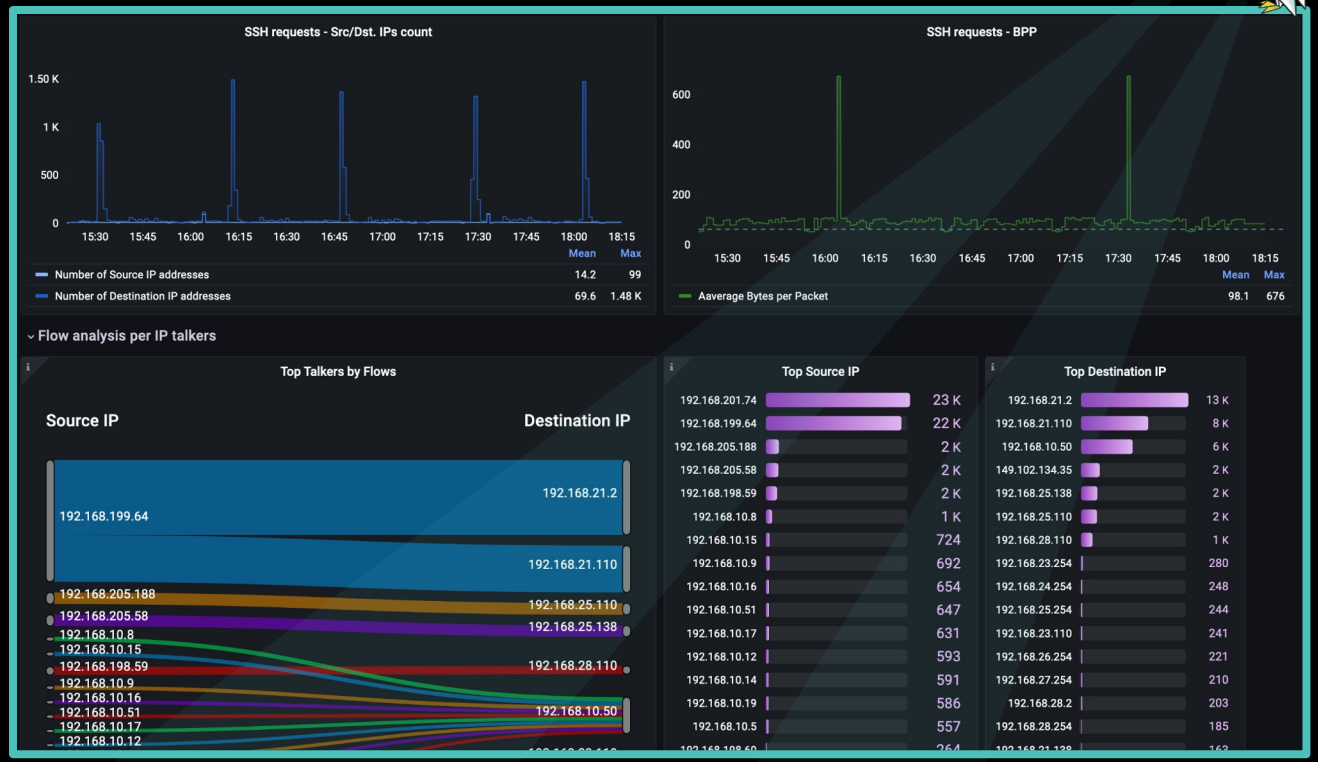
Detection of final attack

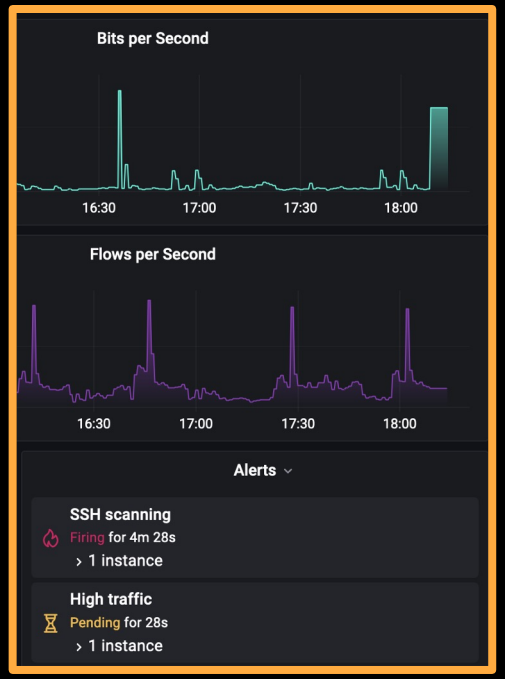
- Attack on OT perimeter
- Attack on DB server credentials

IDS dashboard

FLOWCUTTER

SSH anomaly @ Netflow





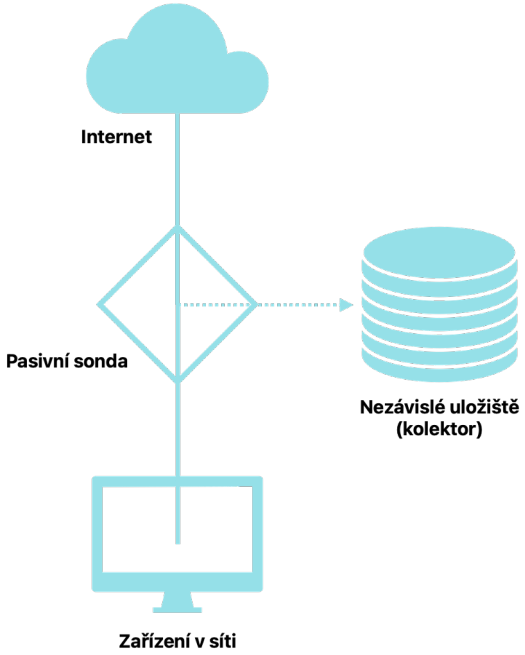
1 alert

2 drill down

FLOWCUTTER

Generating Netflow logs

- Endpoint traces can be tempered
- Netflow is generated independently outside attackers influence
- Netflow logs can be stored elsewhere, (e.g. on collector at other datacenter)



Attacker intercepted

By sheer luck or systematically?

FLOWCUTTER

Incident response

- Hunting w/ logs collection
- Incident reconstruction
- Mitigation
- Posture improvement

Case outcome

Visibility x Blindspots

Photo from Matrix the movie

Visibility X Blindspot

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration

Sources of truth

- NetFlow logs
- Vulnerability scans
- DNS security
- IDS (Suricata)
- IP reputation lists

No application or EDR logs

Mitigation till next day

- Isolate OT & Stop web / db services
- Restrict access to web & db servers (hosted at ISP)
- Update firmware on SME perimeter router & review configuration
- Update firmware on all CORE RouterOS within ISP infrastructure

Case outcome

We see them all

Photo from Matrix the movie

FLOWCUTTER

Improvements after

- Firmware version check in Zabbix for all CORE routers
- Setup more confident anomaly detection (multiple data-sources)
- Fill out blind spots in Netflow coverage
- Update SME perimeter to include firewall w/ dynamic feed
- Setup Suricata in IPS mode on OT perimeter
- Considering EDR / Zero Trust

Case closed

Lessons learnt

FLOWCUTTER

ISP - SME Relationship

- **Initial vector from ISP**
- **Almost delivered costly blow to SME**
- **ISP reacted swiftly and constructively**
- **ISP helped improve security posture**
  (both self & its enterprise customers)

Discussion

Lessons learnt

FLOWCUTTER

5 lessons

- One ⬡ to rule them all
- ???
- ???
- ???
- ???

netflow

Network flow logs

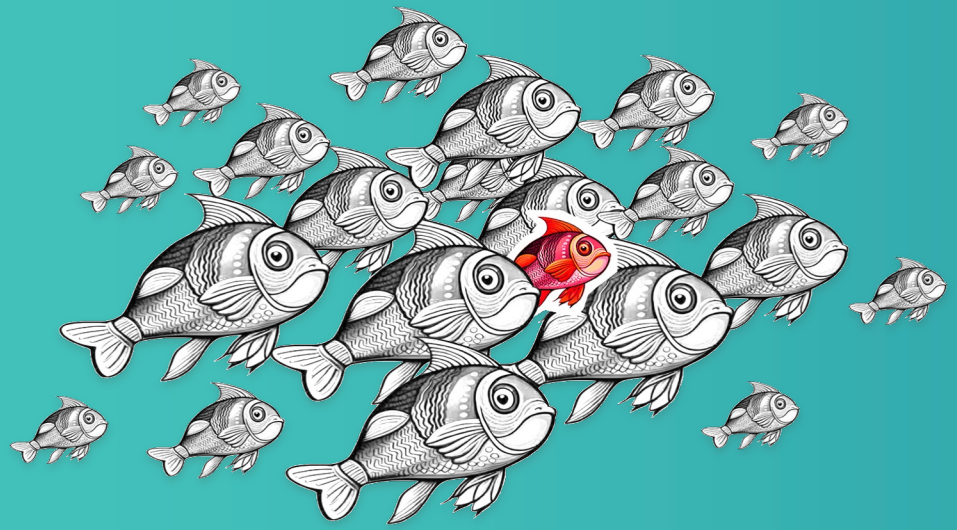
Phto from Matrix the movie

FLOWCUTTER

5 lessons

- One ⬡ to rule them all
- ⬡ is “a must” forensic data source
- ???
- ???
- ???

Anomaly detection



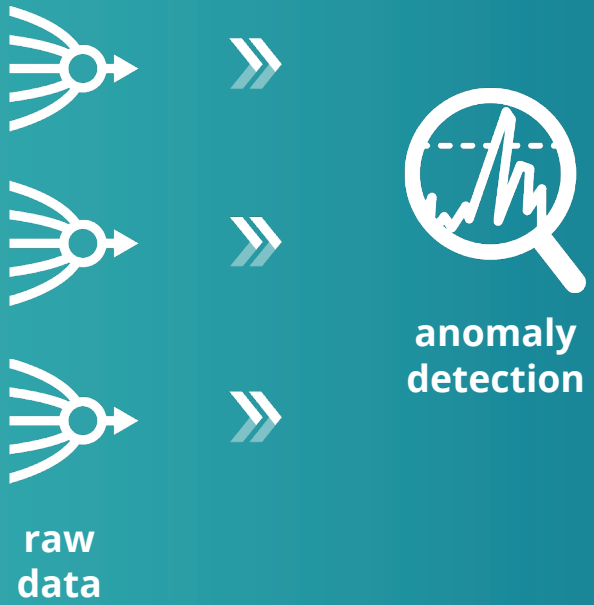


Foto z bluewhale.com

5 lessons

- One ⬡ to rule them all
- ⬡ is “a must” forensic data source
- Networks don’t lie
- ???
- ???

5 lessons

- One ⬡ to rule them all
- ⬡ is “a must” forensic data source
- Networks don’t lie
- Regulatory obligations
- ???

5 lessons

- One ⬡ to rule them all
- ⬡ is “a must” forensic data source
- Networks don’t lie
- Regulatory obligations
- ISP role in security

ISP role

In SME security

Photo from thewertzone.blogspot.com

FLOWCUTTER

Thank you,

ques-tions?

Mgr. Matej Pavelka PhD.

www.flowcutter.com